DOE CIO Guide 205.1-2

U.S. Department of Energy

Cyber Security Program

CERTIFICATION AND ACCREDITATION GUIDE

March 2006

TITLE: CERTIFICATION AND ACCREDITATION GUIDE

1. PURPOSE.

   This Department of Energy (DOE) Chief Information Officer (CIO) Guide provides guidance for the implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*, and the certification and accreditation (C&A) of all information systems within DOE, including the National Nuclear Security Administration (NNSA).

   The DOE CIO will review this guide annually and update it as necessary. DOE Under Secretary and Staff Offices, and their operating units, may provide feedback at any time for incorporation into the next scheduled update.

2. CANCELLATIONS. None.

3. APPLICABILITY.

   a. Primary DOE Organizations. This guidance applies to all DOE Organizations that have access to DOE information and information systems. DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chief Information Officer (CIO), (hereinafter referred to as Senior DOE Management), may also specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their subordinate organizations and contractors (hereinafter called operating units), and for ensuring that those requirements are incorporated into contracts.

   b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE guidance for activities under the NNSA Administrator's cognizance.

   c. National Security Systems. DOE national security systems are required to comply with Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program. E.O. 12829 directed the development of a national security program operating order. Requirements of the *National Industrial Security Program Operating Manual (NISPOM)* and DOE M 471.2-2, *Classified Information Systems Security Manual,* 8-3-99, must be met or exceeded by Senior DOE Management organizations and their operating units when developing, implementing, and assessing appropriate protections for national security systems and classified information.

4. IMPLEMENTATION.

This guide is effective 30 days after issuance. However, DOE recognizes that this guide cannot be implemented into Senior DOE Management PCSPs overnight. Except as noted below, DOE expects that Senior DOE Management shall be in full compliance with the new C&A framework within 90 days of the effective date of this guide. If Senior DOE Management cannot achieve full compliance by the scheduled milestone, DOE expects that Senior DOE Management establish a Plan of Actions and Milestones for implementation of this guide in their PCSP.

5. SUMMARY.

This guide defines the expectations for the certification and accreditation (C&A) process for all information systems in DOE, including NNSA, through the Program Cyber Security Plans (PCSPs).

6. REFERENCES.

References are defined in DOE CIO Guide 205.1-1, *Management, Operation, and Technical Controls*.

7. DEFINITIONS.

Acronyms and terms are defined in DOE CIO Guide 205.1-1, *Management, Operation, and Technical Controls*.

8. CONTACT.

Questions concerning this Manual should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

1. Introduction.

Federal agencies are required to establish a Certification and Accreditation (C&A) process to ensure that adequate security controls are provided for all Department information systems. The proper implementation of the C&A process will ensure that all applicable requirements have been integrated into the development and operational processes. The Department expects that all systems complete C&A prior to going operational, i.e., processing live data or information. This guide describes the minimum expectations for the C&A of information systems within DOE.

This guide is based upon DOE Cyber Security Policy, Federal Information Processing Standard (FIPS) 199, *Standards for the Security Categorization of Federal Information and Information Systems*, FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*, and other applicable Departmental and Federal information technology (IT) security laws and regulations.

2. Purpose.

Utilizing the C&A methodology defined in this guide will result in a standard approach to C&A across DOE. Proper use of the C&A methodology will assure DOE that the level of security controls implemented in an information system adequately protect assets with an acceptable level of residual risk. Senior DOE Management will benefit from the C&A activities performed on their information systems in the following ways:

- Improved understanding of mission risks as they relate to the operation of information systems
- Standard operating environment through utilization of baseline security requirements
- Clearly defined information system boundaries and interconnection agreements between system boundaries
- Documented security plans
- Defined contingency plans
- Established Configuration Management (CM) processes
- Heightened information security awareness
- Validated and monitored security controls
- Measured levels of risk based on identified threats and vulnerabilities

- Uniform General Support System (GSS) and Major Application (MA) inventory (i.e., information sensitivity and mission criticality levels)
- Defined security roles and responsibilities

3. Scope.

This guide includes definition of the C&A process, why C&A is important, description of how C&A maps to the information System Development Life Cycle (SDLC), identification of roles and responsibilities in the C&A process, clarification of types of C&A recommendations and decisions, description of the four phases that comprise the C&A process, and outlining the parts of a complete C&A package.

CHAPTER II

CERTIFICATION AND ACCREDITATION OVERVIEW

1. Certification and Accreditation Overview.

   C&A is the process of formal assessment (certification) and acceptance (accreditation) of system security controls that protect information systems and data stored in and processed by those systems. This process encompasses the system's life cycle and ensures that the risk of operating a system is recognized, evaluated, and accepted. The C&A process implements the concept of "adequate security," or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

   Assessment and test of a system's current security controls determines which controls are in place, implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The System Security Plan (SSP) should detail which security controls are used to meet the security requirements for the information system. Authorizing officials must have the most complete, accurate, and up to date security status information possible in order to make timely, credible, risk-based decisions on whether to authorize system operations.

   A successful C&A process provides Senior DOE Management officials with the necessary assurance that the information system has adequate security controls, that system vulnerabilities have been considered in the risk-based decision to authorize processing, and that appropriate plans and funds have been identified to correct any deficiencies in the information system.

2. System, Type, or Site Accreditation.

   A *system accreditation*, the most common form of accreditation for Major Applications (MA) or General Support Systems (GSS), is an accreditation for a single information system or group of components, network, or MA.

   Type accreditations are used to accredit multiple instances of a MA or GSS for operation at approved locations with the same type of computing environment but the computing environments may be under different management control.

   A *site accreditation* is an accreditation for a particular site or an enclave. A site accreditation is practical with disparate information systems controlled by a single management authority within a well-defined physical site (e.g., region, business center, building, or floor).

3. Importance of C&A.

   Required by OMB Circular A-130, Appendix III, security accreditation provides a form of quality control and challenges managers and technical staffs at all levels to implement the most effective security controls possible in an information system, given mission requirements, technical constraints, operational constraints, and cost/schedule constraints.

   C&A gives Senior DOE Management officials the confidence to explicitly accept the risk to operations, assets, or individuals based on the implementation of an agreed-upon set of defined security controls and the assurance that the system will be operation the appropriate security controls and review throughout its life cycle.

   Responsibility and accountability are core principles that characterize security accreditation. It is essential that Senior DOE Management officials have the most complete, accurate and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems.

   For moderate and high impact systems, as categorized by FIPS 199, the system owner cannot act as the certification agent, therefore, certification agent or designee should be independent of the system development and operations teams. The Senior DOE Management PCSP should specify how the certification agents for their MAs and/or GSSs C&A activities are determined.

4. Accreditation of Large and Complex Systems.

   C&A of large and complex information systems can sometimes be cost-prohibitive and technically infeasible if attempted for the entire system. C&A activities, including funding for C&A, must be established during the development of the information system. Decomposing systems into more manageable multiple components, or subsystems, make this problem more manageable and cost-effective. However, each 'manageable' component or subsystem must be individually certified and accredited.

   When applications and data contained in a MA owned by one organization are hosted on a GSS or transmit data across a GSS network owned by another organization, C&A activities must be coordinated between them. The system owner is responsible for taking the lead on coordination and funding the C&A activities.

   The system owner cannot act as certifier and thus must engage a third party for certification activities. The supporting Senior DOE Management PCSP must specify how the certifiers for their MAs and/or GSSs (information systems) C&A activities are determined.

5. National Critical Infrastructure Information Systems (NCIIS).

   Any information systems designated as critical to the security of the nation, the mission of the Federal government, or directly (i.e., without an intervening information system) supports designated national critical assets in accordance with Presidential Decision Directive 63, *Protecting the Nation's Critical Infrastructure*, are included in this category. If this critical information system requires another information system, (i.e., a MA running on a GSS) for correct operation, then the supporting information system would also be assigned to this category. Categorization of systems that must meet information security requirements for NCIIS are governed by PDD-63, *Practices for Critical Information Assets*, and other applicable Federal and Departmental guidance.

6. Mission Critical Systems.

   Any information system that is determined to be critical to the support of an organization's core missions and goals, and is not a NCIIS, is assigned to this category.

7. Business Essential Systems.

   Any information system whose failure would not preclude organizations from accomplishing core business functions in the long term (more than one month), but would have an impact are included in this category.

8. All other Sensitive Systems.

   All DOE information systems require protection due to the nature of their operation and/or the information they process, store, or transmit, and must meet the basic information security requirements contained in DOE policy and guidance and the applicable Senior DOE Management PCSP.

CHAPTER III

ROLES AND RESPONSIBILITIES

1. Designated Approving Authority (DAA).

The DAA is the Senior DOE Management official who is the *authorizing official* with the authority to formally assume responsibility, and to be held fully accountable, for operating an information system at an acceptable level of risk. This role can be delegated, in writing, to U. S. Government senior management officials within their organization.

Through security accreditation, the DAA assumes responsibility and is accountable for the risks associated with operating an information system. Additionally the DAA may be called upon to:

- Approve system security requirements, system security plans, and memorandums of agreement and/or memorandums of understanding.
- Authorize operation of the information system.
- Issue an interim authorization to operate the information system under specific terms and conditions.
- Deny authorization to operate the information system (or if the system is already operational, halt operations) if unacceptable security risks exist.

Due to the breadth of organizational responsibilities and significant demands on time, a DAA may designate a representative who is empowered to make certain decisions with regard to the planning and resource of the C&A activities.

2. Certification Agent.

The *certification agent* is responsible for conducting a comprehensive assessment of the management, operational, and technical security controls in an information system. The purpose of this assessment is to determine the extent to which controls exist, are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Once the system assessment is complete, the certification agent provides to the Accrediting Official, any recommended corrective actions to reduce or eliminate vulnerabilities in the information system.

To ensure the integrity of the certification assessment, the certification agent should be independent of system development and operations teams as well as those individuals responsible for correcting security deficiencies identified during the certification. The independence of the certification agent ensures the authorizing official receives the most objective information possible in order to make an informed, risk-based, accreditation decision.

3. Information Owner.

   The *information owner* is a DOE official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. Information owners should provide input to information system owners regarding the security requirements and security controls for the information systems where the information resides.

4. System Owner/Program Manager.

   The *information system owner* is the Senior DOE Management operating unit official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

5. Information System Security Officer (ISSO).

   The *information system security officer* is the individual responsible to the authorizing official, information owner, and information system owner for ensuring the appropriate operational security posture is maintained for an information system (GSS or MA). The information system security officer typically has the detailed knowledge and expertise required to manage the security aspects of the information system and is generally assigned responsibility for the day-to-day security operations of the system.

6. System Administrator(s) (SA)

   A system administrator (SA) is a privileged user who has access to system control, monitoring, or administration functions and is responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established information security policy and procedures.

7. User Representative.

   Users, at all levels of an organization, are responsible for the identification of mission/operational requirements and for complying with the security requirements and security controls described in the SSP. *User representatives* are individuals that represent the operational interests of the user community and serve as liaisons for that community throughout the information system development life cycle.

CHAPTER IV

CERTIFICATION AND ACCREDITATION PROCESS

1. Introduction.

   This section establishes a common approach for the specific tasks and subtasks required to complete the C&A of an information system, in accordance with OMB Circular A-130, Appendix III, and derived from guidance published in NIST SP 800-37.

2. Phases of C&A.

   There are four (4) major phases to the C&A methodology:

   - Initiation Phase. Establishing security requirements, C&A boundary, schedule, level of effort, and resources required.
   - Certification Phase. Conducting a security assessment of controls, documenting residual risks, and producing the final documents for the C&A package to support the authorizing official in making an informed accreditation decision.
   - Accreditation Phase. Evaluating the residual risk, making the accreditation decision, and documenting the decision as part of the C&A package.
   - Continuous Monitoring Phase. Ensuring the continued operation and maintenance of the system to preserve an acceptable level of residual risk

3. Elements of C&A Package.

   The output of the C&A process is a number of elements designed to convey to the authorizing official the security posture and the level of residual risk associated with the information system. Documentation generated by the C&A process must include:

   a. Certification:

   - System Categorization – The System Security Plan, or an attachment to the plan, must include the security category for the information system based on the impact level for each security objective (confidentiality, integrity, and availability) as described in FIPS 199. The applicable Senior DOE Management PCSP, DOE Guide 205.1-1, *Management, Operation, and Technical Controls*, and NIST SP 800-60 provide further guidance. The Senior DOE Management PCSP will specify the process for system categorization.
   - Approved System Security Plan – An SSP must be developed and implemented for all MAs and GSSs. The SSP provides an overview of the system impact level, types of information processed, security requirements for the system, and a description of the security controls in place or planned for meeting those requirements. The SSP

provides information necessary to secure an information system throughout its life cycle. However, the SSP need not contain all security documentation; it may be part of a hierarchy of security documents. Designated officials within the organization review and approve the SSP. The Senior DOE Management PCSP will specify any required format of the SSP.

- Completed Security Risk Assessment - DOE requires that every operating unit have a risk management process in place that follows the methodology and reporting format defined by the Senior DOE Management PCSP and DOE Guide 205.1-3, *Risk Management*. The family of security controls in DOE Guide 205.1-1, *Management, Operation, and Technical Controls*, called Risk Assessment (RA) provides further guidance in this area. The Senior DOE Management PCSP will specify any required format of the risk assessment statement.
- Configuration Management Plan - DOE expects that organizations ensure that information system developers create and implement a methodology that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the methodology and its implementation. Senior DOE Management PCSP and DOE Guide 205.1-8, *Configuration Management*, provides further guidance in this area.
- Contingency Plan - Contingency planning details the necessary procedures required to protect the continuing performance of core business functions and services, including information services, during an outage. Senior DOE Management and DOE guidance, DOE Guide 205.1-7, *Contingency Planning*, provides further guidance in this area.
- Security Test & Evaluation Report – A comprehensive evaluation (System Test and Evaluation [ST&E]) of all the management, operational and technical security controls for the information system must be conducted to determine:

  1. The effectiveness of those controls in a particular environment of operation; and
  2. The vulnerabilities in the system after the implementation of such controls.
  3. NOTE: For LOW impact systems, a self-assessment can be substituted for a ST&E.

  The Senior DOE Management PCSP provides describes ST&E activities and format of the ST&E report.

- Interconnection Security Agreements - DOE expects that the system owner authorize all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. The Department expects DOE expects that system owners utilize the methodology for documenting system support and interconnectivity agreements as developed in accordance with the applicable PCSP and DOE Guide 205.1-5, *Interconnection Agreements*.

- Completed Privacy Impact Assessments - DOE expects that the operating units conduct a privacy impact assessment on applicable information systems. The Senior DOE Management PCSP will specify any required format of the privacy impact assessment.
- Plan of Action and Milestones - DOE expects that the operating units develop and regularly update, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. The Senior DOE Management PCSP and DOE Guide 205.1-6, *Plan of Action & Milestones (POA&M)*, provides further guidance in this area.
- Security Assessment Report (SAR)[1] - A SAR is prepared and signed by the certification agent referencing the complete certification documentation package. The report provides (i) the results of assessing the security controls in the system to determine the extent to which the controls are implemented correctly and operating as intended, and producing the desired outcome with respect to meeting the system security requirements; (ii) recommendations for correcting deficiencies in the security controls and reducing or eliminating identified vulnerabilities, and (iii) recommendation to the Accrediting Official regarding accreditation. The Senior DOE Management PCSP will specify any required format of the SAR.

b. Accreditation:

- Accreditation decision letter - The accreditation decision letter transmits the authorizing official's accreditation decision. The authorizing official attaches the certification documentation to the original accreditation decision letter to complete the Accreditation Package and returns the Accreditation Package to the information system owner. The Senior DOE Management PCSP will specify any required format for the accreditation letter.

[1] Typically referred to as a Certification Letter.

CHAPTER V

INITIATION PHASE

1. Introduction.

   The Initiation phase allows an organization to quickly determine the information system security status and what changes have to be made to bring it back or keep them in compliance with the Senior DOE Management PCSP, DOE guidance and other Federal requirements. The initiation phase is comprised of three tasks:

   - Preparation
   - Notification and Resource Identification
   - System Security Plan Analysis, Update and Acceptance

2. Preparation.

   The preparation task examines the SSP and confirms that the contents of the plan are consistent with an initial assessment of risk.

   The preparation task is broken down into six sub tasks:

   - Information System Description – The Information System Owner confirms that the information system has been fully described and documented in the SSP.
   - Security Categorization – The Information System Owner confirms that the information system has been categorized according to the applicable PCSP, FIPS 199, and documented in the SSP.
   - Threat Identification – The Information System Owner confirms that potential threats have been identified and documented in the SSP.
   - Vulnerability Identification – The Information System Owner confirms that vulnerabilities to the system have been identified and documented in the Risk Assessment in accordance with the requirements in the applicable PCSP and DOE Guide 205.1-3, *Risk Management*.
   - Security Control Identification – The Information System Owner confirms that the security controls both implemented and planned are documented in the SSP.
   - Initial Risk Determination – The Information System Owner confirms that all risks have been identified and documented in the Risk Assessment.

3. Notification and Resource Identification.

   The Notification and Resource Identification task provides Senior DOE Management with a warning that a C&A is being accomplished. Resources are then identified along with a Plan of Actions and Milestones (POA&M) for the C&A activities.

   The preparation task is broken down into two sub tasks:

   - Notification – The Information System Owner notifies all stakeholders that a C&A is to be accomplished.
   - Planning and Resources – The Information System Owner determines the level of effort and corresponding resources needed to accomplish the C&A. A POA&M is then drafted for execution.

4. SSP Analysis, Update and Acceptance.

   The SSP Analysis, Update and Acceptance task requires an independent review of the security categorization, an analysis of the SSP, an update to the SSP and a formal acceptance of the SSP by the authorizing official.

   This task is broken down into four sub tasks:

   - Security Categorization Review- An independent review by the authorizing official, ISSO, and certification agent of the security categorization documented in the SSP must take place.
   - System Security Plan Analysis - An independent review by the authorizing official, ISSO and certification agent of the SSP to determine if the documented vulnerabilities and associated risks are accurate.
   - System Security Plan Update – The Information System Owner updates the SSP with any findings from the independent Security Categorization Review and SSP Analysis.
   - System Security Plan Acceptance – The authorizing official reviews the SSP to determine if the documented risks are acceptable.

CHAPTER VI

CERTIFICATION PHASE

1. Introduction.

The Certification phase demonstrates, through independent validation using selected verification techniques and procedures, the security controls for the information system have been implemented correctly and are effective in their application. Correct and effective implementation of security controls is a necessary condition to demonstrate compliance with the information system security requirements. The results of the certification phase are documented in the Security Assessment Report (SAR), which are included in the final certification package along with the other documents from the Initiation phase. The certification phase consists of two tasks:

- Security control assessment
- Certification documentation

2. Security Control Assessment.

The purpose of this task is to prepare, conduct and document an accurate assessment of the security controls.

This task is broken down into four sub tasks:

- Documentation and Supporting Materials – The Information System Owner and the Certification Agent compile all relevant documentation and materials needed for the security control assessment.
- Methods and Procedures – The Certification Agent selects or develops procedures to perform an assessment of the security controls. The Senior DOE Management PCSP defines the appropriate methodology for assessment of the security controls.
- Security Assessment – The Certification Agent performs an audit of the security controls in place. The Senior DOE Management PCSP describes the requirements for conducting the security assessments.

3. Certification Documentation.

The purpose of this task is to provide the certification findings to the information system owner, update the SSP as needed, prepare the POA&M, and assemble the accreditation package.

This task is broken down into four sub tasks:

- Findings and Recommendations – The Certification Agent captures the results of the Security Assessment by identifying the controls in place, that they are implemented correctly and operating as intended. It further makes recommendations for correcting the deficiencies or reducing and/or eliminating vulnerabilities. The SAR is part of the final accreditation package. The Certification Agent provides the information system owner with the SAR.
- System Security Plan Update – The Information System Owner updates the SSP based on the security assessment and any modifications to the security controls.
- Plan of Actions and Milestones – The Information System Owner puts together a POA&M that outlines the milestones and schedule for addressing the issues and recommendations identified in the SAR.
- Certification Package Assembly – The Information System Owner assembles the final certification package and submits it to the authorizing official. The package includes: the documents from the Initiation phase, including Certification phase updates, the SAR, and POA&M.

.

CHAPTER VII

ACCREDITATION PHASE

1. Introduction.

The purpose of the accreditation phase is to decide if the remaining vulnerabilities pose an acceptable level of risk. The decision can be an authorization to operate, an interim authorization to operate or a denial of authorization to operate. The accreditation phase consists of two tasks:

- Accreditation decision
- Accreditation documentation

2. Accreditation Decision.

The purpose of this task is to determine all of the risks and whether the level of risk is at an acceptable level.

This task is broken down into two sub tasks:

- Final Risk Determination – The authorizing official determines the overall risk based on the evidence presented in the final certification package.
- Risk Acceptability – The authorizing official determines the residual risk is at an acceptable level. A final accreditation decision letter is then prepared

3. Accreditation Documentation.

The purpose of this task is to create and disseminate the final accreditation package.

This task is broken down into two sub tasks:

- Accreditation Package Transmission – The authorizing official provides copies of the final accreditation package with original accreditation decision letter to the Information System Owner.
- System Security Plan Update – The Information System Owner updates the SSP with the results of the accreditation process.

CHAPTER VIII

CONTINUOUS MONITORING PHASE

1. Introduction.

The purpose of the Continuous Monitoring phase is to provide oversight and monitoring of security controls on an ongoing basis. This phase consists of three tasks:

- Configuration Management and Control
- Security Control Monitoring
- Status Report and Documentation

2. Configuration Management and Control.

The purpose of this task is to document and assess proposed and actual changes to the information system.

This task is broken down into two sub tasks:

- Documentation of the Information System Changes – The Information System Owner documents the proposed and actual changes to the system.
- Security Impact Analysis – The Information System Owner analyzes proposed or actual changes to the system to determine the security impact.

3. Security Control Monitoring.

The purpose of this task is to select the set of controls to be monitored and periodically assess those controls.

This task is broken down into two sub tasks:

- Security Control Selection – The Information System Owner selects the security controls to be monitored on a continuous basis.
- Selected Security Control Assessment – The Information System Owner assesses the controls designated to be continuously monitored.

4. Status Report and Documentation.

The purpose of this task is to update the SSP to reflect changes, update the POA&M based on the Continuous Monitoring activities and report the security status of the information system to the authorizing official.

.

This task is broken down into three sub tasks:

- System Security Plan Update – The Information System Owner updates the plan with changes identified from the Continuous Monitoring activities and begins the Certification phase.
- Plan of Action and Milestones Update – The Information System Owner updates the POA&M based on the results of the Continuous Monitoring activities.
- Status Reporting – The Information System Owner reports the security status of the information system to the authorizing official.

ATTACHMENT 1:

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH GUIDE 205.1-2 IS APPLICABLE

Office of the Secretary

Chief Information Officer

Departmental Representative to the Defense Nuclear Facilities Safety Board

Energy Information Administration

National Nuclear Security Administration

Office of Civilian Radioactive Waste Management

Office of Congressional and Intergovernmental Affairs

Office of Counterintelligence

Office of Economic Impact and Diversity

Office of Electric Transmission and Distribution

Office of Energy Assurance

Office of Energy Efficiency and Renewable Energy

Office of Environment, Safety and Health

Office of Environmental Management

Office of Fossil Energy

Office of General Counsel

Office of Hearings and Appeals

Office of Intelligence

Office of Legacy Management

Office of Management, Budget and Evaluation and Chief Financial Officer

Office of Nuclear Energy, Science and Technology

Office of Policy and International Affairs

Office of Public Affairs

Office of Science

Office of Security and Safety Performance Assurance

Office of the Inspector General

Secretary of Energy Advisory Board

Bonneville Power Administration

Southeastern Power Administration

Southwestern Power Administration

Western Area Power Administration

.